



Bank Spółdzielczy w Jordanowie

Rok założenia 1880

www.bsjordanow.pl

Podstawowe zasady bezpieczeństwa korzystania z bankowości elektronicznej

Wprowadzenie

Twoje pieniądze i dane w banku są cenne. Bank chroni je swoimi systemami, ale Ty też masz bardzo ważną rolę. Jeśli nie będziesz uważać, oszuści mogą przejąć Twoje konto, wykraść pieniądze albo dane osobowe.

Dlatego zawsze stosuj się do poniższych zasad:

1. Chroń telefon i dane do logowania

Twój telefon to „klucz” do konta – bo masz na nim SMS-y z kodami i aplikację mobilną.

Nigdy nie podawaj nikomu loginu, hasła ani kodu BLIK – nawet rodzinie czy znajomym.

Oszuści potrafią podszyć się pod Twoich znajomych i prosić o kod.

Jeśli ktoś prosi o kod BLIK – zawsze zadzwoń i upewnij się, że jest to znana Tobie osoba.

Co się może stać, jeśli nie sprawdzisz? Oszuści w kilka minut wypłacą Twoje pieniądze z bankomatu albo zapłacą nimi w sklepie.

2. Upewnij się, że logujesz się na stronę Banku

W przypadku:

- Przeglądania strony internetowej Banku w pasku adresu zawsze musi być kłódka i adres dokładnie o treści <https://bsjordanow.pl>;
- logowania się na stronę bankowości internetowej eBankNet w pasku adresu zawsze musi być kłódka i adres dokładnie o treści <https://ebank.bsjordanow.pl>;
- logowania się na stronę bankowości korporacyjnej eCorpoNet w pasku adresu zawsze musi być kłódka i adres dokładnie o treści <https://ekorp.bsjordanow.pl>.

Kliknij kłódkę i sprawdź certyfikat.

Nigdy nie loguj się przez link z SMS-a czy e-maila.

Dlaczego? Fałszywe strony wyglądają jak prawdziwe, ale kradną Twoje dane - różnice w treści mogą być prawie niewidoczne.

3. Logowanie i hasła

Do logowania podajesz tylko identyfikator, kilka znaków hasła i kod SMS/aplikacji.

Zmieniaj hasło regularnie i nie używaj go w innych serwisach.

Dlaczego? Jeśli ktoś pozna Twoje hasło z innej strony, może spróbować użyć go w Banku.

4. Ostrożnie z wiadomościami i linkami

Nie otwieraj podejrzanych e-maili i SMS-ów.

Nie otwieraj podejrzanych linków w otrzymanych wiadomościach e-mail i SMS.

Nie pobieraj załączników otrzymanych w wiadomości e-mail od nieznanych osób.

Przykład: dostajesz fałszywą fakturę, a po otwarciu wirus powoduje przekierowanie Twojego przelewu do złodzieja.

5. Nigdy nie instaluj programów do „pomocy zdalnej”

Oszuści udają pracowników Banku i proszą o instalację TeamViewer lub AnyDesk.

Dzięki nim mogą przejąć Twój komputer.

Pamiętaj: Bank nigdy nie prosi swoich Klientów o instalację programów do zdalnej pomocy!

6. Dbaj o bezpieczeństwo urządzeń

Zainstaluj i aktualizuj antywirusa.

Aktualizuj system, przeglądarkę internetową i aplikacje.

Regularnie skanuj komputer i telefon.

Dlaczego? Skanowanie pozwala wykryć wirusy i w porę uniknąć problemów! Aktualizacje łatają dziury w systemie, które mogą wykorzystać oszuści!

7. Sprawdzaj przelewy

Zawsze porównuj dane w SMS-ie/aplikacji z tym, co wpisałeś.

Sprawdzaj numer telefonu przy przelewach BLIK.

Najlepiej wpisuj numery kont ręcznie – wirusy potrafią podmienić je w schowku.

Cyklicznie sprawdzaj, czy numery rachunków w przelewach zdefiniowanych nie uległy podmianie – aby uniknąć sytuacji, że chciałeś wysłać pieniądze znajomemu, a trafiły do złodzieja.

8. Kontroluj konto

Regularnie przeglądaj historię rachunku i operacji na swojej karcie płatniczej pod kątem podejrzanych transakcji.

Zwracaj uwagę nawet na małe podejrzane przelewy – to może być test przeprowadzany przez oszusta.

9. Unikaj publicznego Wi-Fi

Nie loguj się do Banku przez darmowe Wi-Fi (np. Na stacji benzynowej), lub hotelu, kawiarni.

Dlaczego? Oszuści mogą podglądać dane w takich sieciach.

10. Reaguj natychmiast

Jeśli coś jest podejrzane – od razu dzwoń do Banku:

Tel. 18 267 55 20 (pn.–pt. w godzinach od 7:00 do 16:30)

E-mail: jordanow@bsjordanow.pl

11. Limity operacji

Ustaw limity przelewów i wypłat.

Dlaczego? Nawet jeśli ktoś przejmie konto, kradzież będzie bardziej czasochłonna i wymagała wykonania wielu operacji.

12. Bank nigdy nie pyta o...

- Hasła, kody BLIK ani inne poufne dane.
- Linki do logowania.
- Instalację dodatkowych programów.

Jeśli dostaniesz takie wiadomości – to oszustwo!

13. Nietypowe wiadomości

Bank nie wysyła dziwnych próśb o instalację programów.

Jedynymi wyjątkami są aplikacja mobilna i e-podpis.

14. Wylogowanie

Po zakończeniu korzystania z bankowości internetowej/ aplikacji mobilnej zawsze klikaj „Wyloguj”.

Dlaczego? To zamyka sesję połączenia z Bankiem i chroni Twoje konto.

15. Znaj aktualne zasady bezpieczeństwa

Zapraszamy do zapoznania się z materiałami dotyczącymi bezpieczeństwa w sieci zamieszczonymi na stronie internetowej Banku pod adresem:

<https://bsjordanow.pl/bezpieczenstwo-w-bankowosci-internetowej>

Sprawdź także zasady bezpieczeństwa na stronie: zbp.pl/dla-klientow/bezpieczne-bankowanie/bankowosc-internetowa

Dlaczego? Oszuści stale zmieniają pomysły na sposoby ataku!

16. Fałszywe przelewy

Jeśli dostaniesz potwierdzenie przelewu, którego nie robiłeś – natychmiast dzwoń do Banku.

Dlaczego? Może uda się nam go zatrzymać.

17. Filtrowanie IP

W przypadku eCorpoNet możesz ustawić logowanie tylko z wybranych adresów internetowych (np. z domu).

Dlaczego? Dzięki temu nikt obcy się nie zaloguje...

18. Urządzenia zaufane

Jeśli chcesz dodać urządzenie do zaufanych, urządzenie musi być Twoje, z antywirusem i aktualnym systemem operacyjnym.

Dodanie urządzenia do zaufanych powoduje, że Bank nie będzie Ci wysyłał SMS-ów przy logowaniu.

Dlaczego? Urządzenie dodane do zaufanych powinno być dobrze zabezpieczone, jest ono “kluczem” do Twojego konta.

19. Blokada dostępu

Możesz sam zablokować konto w opcji „Zablokuj dostęp” w systemie eBankNet.

Działa 24/7 i jest darmowa.

Dlaczego? Jeśli podejrzewasz, że ktoś obcy próbuje dostać się do Twojego konta, możesz szybko zablokować dostęp i ochronić swoje pieniądze.

20. Używane oprogramowanie

Zadbaj, aby każde używane oprogramowanie pochodziło z legalnego i zaufanego źródła.

Podsumowanie

Jeśli nie będziesz przestrzegać zasad, ktoś może przejąć Twoje konto, ukraść pieniądze i dane osobowe.

Twoje bezpieczeństwo zależy od Ciebie. Jeśli masz wątpliwości – zawsze dzwoń do Banku.